UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

ANAS ELHADY, *et al.*,	)	
	)	**Case No. 16-cv-00375**
Plaintiffs,	)	**Hon. Anthony J. Trenga**
	)	**Hon. Mag. John F. Anderson**
	)	
v.	)	RE-FILED PUBLICLY PURSUANT
	)	TO COURT ORDER (Dkt. 295)
CHARLES H. KABLE, Director of the Terrorist Screening Center; in his official capacity, *et al.;*	)	
	)	
Defendants.	)	

PLAINTIFFS' SUPPLEMENT TO THEIR MOTION TO COMPEL COMPLIANCE WITH THE COURT'S FEBRUARY 22 ORDER

Minutes before Plaintiffs filed their March 1st Motion to Compel, Defendants provided two additional supplements describing the federal government's private dissemination practices. These supplements came following a week of counsels' telephonic meet-and-confers and in-person meetings regarding compliance with this Court's February 22, 2019 order requiring Defendants to disclose more information regarding the federal government's private dissemination practices. *See* Dkt. 271. Plaintiffs were not able to read Defendants' supplemental discovery responses prior to filing their motion to compel, which was based on viewing Defendants' private entity list. Accordingly, as previewed in their Friday motion (*see* Dkt. 279 at 4), Plaintiffs hereby provide a supplement to their motion to compel regarding the items remaining in dispute.

Plaintiffs' counsel acknowledges and expresses their appreciation that Defendants' supplemental responses address several of Plaintiffs' counsel's general and specific inquiries regarding the FBI's role in disseminating TSDB information to private entities.

Counsel further acknowledges that, following their review, most of the private entity list matches Defendants' representations regarding access by private correctional facilities, private police and security forces for railroads, universities, and hospitals, and the like.

There are, however, revealing exceptions. The presence of these exceptions, and the lack of explanations for them in Defendants' supplement, heightens Plaintiffs' need for further information regarding Defendants' private dissemination practices. These exceptions are not consistent with the various government declarations and thus prevent the Plaintiffs from fully relaying to Judge Trenga how the federal government's private dissemination practices work.

For example, Defendants' discovery supplement provides more details about the federal and state telecommunication networks that supply access to the NCIC. *See* CJIS Supplemental Response, Exhibit A at 5. Defendants' supplement represents that "NCIC is not web-based and is not available or accessible on the internet." *Id.* at 5. However, one private data processing provider on the list touts on its website its new mobile app, which provides end users with instant access to law enforcement databases via the internet. Another set of authorized-access NCIC entities are single-person private investigator and process server firms located within a single state. It thus seems like, at least in that state, the hardware and networks provided may just be these process servers' personal laptops with internet connections.

Defendants' discovery supplements further set forth the legal limitations they place on complex corporate entities using the NCIC for purposes other than those that regard criminal justice. The defendants also disclose a Defendant-driven process for identifying and rectifying misuse. *Id.* at 5-6.

However, Defendants provide no information regarding either how commonly such misuse occurs, or what technical (as opposed to legal) measures prevent the misuse. For example, what technically stops the single-person private investigator identified above from using his personal access to the NCIC for both permissible and impermissible purposes? What technical measures, if any, automatically flag (akin to a fraudulent credit card purchase) a query that looks suspicious? As another example, last week one state decertified a major private university police force due to that police force's history of improperly sharing law enforcement records with the university's separate honor code office, and the university police force's subsequent failure to comply with public records requests. The scandal had begun with stories of students expelled for off-campus conduct, including one who was the victim of sexual assault, which conduct the university had learned about through police channels. With state decertification pending, will that university police force's ORI be revoked at the federal level in turn? Defendants refer to an "audit review" and other "corrective measures" to address such misuse, as well as a biennial continuing "validation" process, but the details are ambiguous. *See* Ex. A at 6.

The discovery supplement provides some specific answers regarding private entities on the list which Plaintiffs' counsel flagged. For example, the supplement explains how animal welfare organizations may have law enforcement divisions with access to the NCIC. *See* Ex. A at 4. (This addresses Plaintiffs' counsel's "animal shelter" concern raised in Friday's motion.) Defendants' supplement also addresses some ambiguities in the list, pursuant to which universities themselves and not a "University PD" had been designated. *See* Ex. A at 7-8. (This addresses Plaintiffs' Friday motion concern, regarding ambiguity in university names.) And Defendants' supplement expands the list of categories of private

entities with access to include, for example, a few private police departments for an airport, transportation authority, and unincorporated communities. But this expanded category list still leaves several material gaps, based on Plaintiffs' counsel's research during live viewings last week.

Specifically, Plaintiffs' counsel believes that the following material gaps remain in Defendants' description of its private dissemination practices:

A church police department. One entity on Defendants' list is a Midwestern church which touts several megachurch "campuses." These "campuses" are not universities; they are additional church buildings. The church appears to operate just one private K-12 school at one church "campus" location. The authorized ORI appears to go to a private security force that protects the church itself, although plaintiffs struggled to find any public record of that security force's existence. The nature of the church is such that Defendants could not possibly issue it an ORI consistent with 28 U.S.C. § 534(e), regarding university police force access.

High schools. Two other entities on the list are also private security forces for high schools, not universities. To the extent these entities were authorized under 28 U.S.C. § 534(e) as universities, this also appears to be error.

Steel mill. One entity on the list is a major rust belt, and international, steel manufacturer. Plaintiffs' counsel has not yet seen any explanation as to how this large corporation, or its private security force in the Midwest, qualifies for NCIC access.

Global security service. One private security corporation is listed as an ORI, although the ORI as named is limited to just one office location which provides services to one city. Nevertheless, this corporation operates around the world and touts its Fortune

500 clientele. Plaintiff's counsel requests examination of this specific contract, in order to ensure that the single-city access has not served as an entry point for worldwide corporate dissemination.

Halfway houses and substance abuse centers. Although they appear to fall under Defendants' rubric of private probational services, Plaintiffs assert that additional information about several of these centers must be disclosed. One was bought out after a state investigation found it engaged in predatory and abusive practices, yet its ORI's remain. Another touts its use of data to provide predictive assessments for bail and release conditions. Another engages in widespread electronic monitoring of its clientele, including GPS bracelets and alcohol monitoring. Several have almost no internet footprint, and in at least one case the center is reported as having been closed. The wide range of services, of varying rigor and quality, by these private probation center, concerns Plaintiff's counsel about their potential for abuse of watchlist records.

Counsel cannot be more specific regarding the issues that emerged from the Defendants' private entities list without violating the Court's order to not write or type the private entity names in any form. *See* Dkt. 274. Plaintiffs believe review of these examples *in camera* with the Court will prove illustrative of the wide gaps in Defendants' description of its private dissemination practices.

A CORRECTION

In addition to the points regarding animal welfare organizations and unclear university names referenced above, which were characterized in Plaintiff's Friday motion but addressed by Defendant's counsel, Plaintiff's counsel offers one more correction. In Friday's motion, Plaintiffs' counsel referred to NCIC access by "a veterans-oriented

foundation." This was a mistake. Defendants clarified during one of last week's live viewings that this listed entity was actually a public, not a private, entity related to veterans, and thus should not have been on the list at all.

However, this correction, alongside Defendants' deduplication and narrowing of the list (*see* Exhibit B – TSC Supplement) and Defendants' representations that 145 public city attorney's offices (Ex. A at 2 n.3) "were mistakenly included on the List," heightens Plaintiffs' counsel's concerns that the opposite may also be true. Namely, that hundreds of entities classified as having "public" access to the NCIC may currently be mis-designated, and actually represent private entities.

RELIEF REQUESTED

Plaintiffs respectfully request an *in camera* hearing where counsel for all parties and the Court may have the private entities list in front of them. This would allow Plaintiffs the opportunity to fully present their views as to the issues that arose upon review of Defendants' private entity list. Defendants' counsel has been helpful in providing more specific information upon request, but the parties appear to have a fundamental disagreement about the nature of some of the entities, and about various aspects of Defendants' private dissemination practices. Plaintiffs' counsel are barred from conducting further research outside of Defendants' facilities.

As detailed in Plaintiffs' opening motion (Dkt. 279 at 2-3), Plaintiffs also continue to seek an opportunity for Shereef Akeel, the senior trial lawyer on the case, to view the private entity list at a government office. In light of the substance of Defendants' supplement, however, Plaintiffs clarify their request for further relief to the following:

(1) Defendants' commitment to reducing all information they prepared and vetted about the private dissemination list, executive-level information about private

dissemination practices, and individual entries on that list to an admissible form. Defendants provided many specific descriptions to Counsel during meet-and-confer that are not incorporated into their discovery supplement. This information would remain AEO.

(2) A blank ORI application, or if more than one is in use, all blank ORI applications;

(3) Basic statistics regarding the number of ORI applications received, accepted, rejected, and modified;

(4) Boilerplate government contracts Defendants use with ORI's, as well as 10 executed contracts regarding ORI's that, in Plaintiffs' view, are of top-tier concern;

(5) A log of every ORI's signed acknowledgment form that Defendants assert establishes meaningful and effective limits on access and us of TSDB information;

(6) Executive-level information regarding what Defendants know about whether any legal and technical rules which exist on access and use of TSDB information are followed.

Respectfully submitted,

COUNCIL ON AMERICAN-ISLAMIC RELATIONS

BY: /s/ Gadeir Abbas
LENA F. MASRI (DC 1000019) (pro hac vice)
GADEIR I. ABBAS (VA 81161)*
CAROLYN M. HOMER (DC 1049145) (pro hac vice)
Attorneys for Plaintiffs
453 New Jersey Ave, SE
Washington, DC 20003
Phone: (202) 742-6420

**Gadeir Abbas is licensed in VA, not in D.C. Practice limited to federal matters.*

AKEEL & VALENTINE, PLLC
SHEREEF H. AKEEL (P54345)
888 W. Big Beaver Rd., Ste. 910
Troy, MI 48084
Phone: (248) 269-9595
shereef@akeelvalentine.com

Dated: March 4, 2019 (refiled March 8, 2019 per Court Order)

CERTIFICATE OF SERVICE

I hereby certify that on March 8, 2019, I electronically filed the foregoing by using the Court's ECF system. I certify that all counsel will receive copies through the ECF system.

/s/ Gadeir I. Abbas

Exhibit A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

ANAS ELHADY, et al.	)	
Plaintiffs,	)	
v.	)	Case No. 1:16-cv-375
CHARLES H. KABLE, et al.	)	
Defendants.	)	

CJIS SUPPLEMENTAL RESPONSE

Interrogatory 30: Identify all information TSC possesses that indicates for-profit companies received TSDB information.

Supplemental Response:

At the February 22, 2019 hearing in the above-captioned matter, the Court ordered the Defendants to commemorate certain information that defense counsel had relayed to Plaintiffs' counsel on behalf of the staff of the Operational Programs Branch (OPB) of the Criminal Justice Information Services (CJIS) Division of the FBI, in connection with the list of Originating Agency Identifiers (ORIs)[1] that plaintiffs' counsel viewed in accordance with the Court's February 22, 2019 order ("the List"), in a supplemental response. To that end:

No private entity can receive an ORI unless it can demonstrate that it is either (a) an authorized railroad or college/university police department, pursuant to 28 U.S.C. § 534(e), or (b) is providing services on behalf of or in support of (i) a criminal justice agency (CJA), as set forth in 28 C.F.R. § 20.3(b)(7), or (ii) a noncriminal justice agency performing criminal justice

[1] An ORI is a multi-character alphanumeric identifier assigned by NCIC to an agency or entity in order to identify it in transactions on the NCIC System.

dispatching functions or data processing/information services for CJAs, as set forth in 28 C.F.R. § 20.3(b)(6), and submits the required documentation demonstrating its eligibility.[2] Each private entity on the List satisfies the requirements set forth in the February 20, 2019 Rago declaration, although a few listed entities have been subsequently determined to be governmental entities.[3] As explained in the first Supplemental Response to Interrogatory 30 and in my declaration, the number of qualified private entities is less than 1441, because in many instances, multiple ORIs have been issued to the same entity. Since the first Supplemental Response, after accounting for duplicate entries on the list of ORIs that plaintiffs' counsel viewed in accordance with the Court's February 22, 2019 order ("the List"), the FBI now approximates the number of qualified private entities to which ORIs have been issued to be approximately 533.[4]

Decisions to grant or deny an ORI, which is needed to gain National Crime Information Center (NCIC) access, are made by staff in the FBI CJIS OPB. The FBI does not seek out private entities to apply for NCIC access; rather, those private entities apply for access. Typically, the law enforcement or criminal justice agency with which the private entity has an

---

[2] Henceforth, this statement refers to these entities collectively as "qualified private entities," or "the private entities."

[3] City Attorney's offices sometimes contract with private attorneys; accordingly, where a private attorney is in a qualified agreement with a CJA (i.e. a City Attorney's office), it is properly included on the List. However, in the course of further conferrals with Plaintiffs regarding the List, it became apparent that a certain limited number of City Attorney entities, 145 to be exact, were mistakenly included on the List, when in fact those City Attorney entities are government agencies. Likewise, upon further review, three other entities that were on the List were determined to in fact be governmental entities.

[4] In identifying duplicates, the FBI consolidated entities that had the exact entity name and the same state of operation, as well as slight variations on the entity name (e.g. ABC Railroad Police Department and ABC Railroad PD) but the same state of operation. The same entity, such as ABC Railroad, operating in multiple states, was still counted multiple times, in other words, once for each state of operation. If such entities operating in multiple states were not counted separately for each state, the number of qualified private entities would be lower, approximately 453.

agreement contacts the state CJIS Systems Officer (CSO) on behalf of the private entity, to request an ORI. The state CSO passes the ORI request along to the FBI CJIS Division only if the state CSO finds that the application meets all of the criteria for ORI eligibility. In other words, the state CSO can decline the application before it is ever sent on to the FBI.

The employees at qualified private entities that have access to the NCIC use any information they obtain from an NCIC query the same way a law enforcement entity would—for law enforcement purposes. For example, if an authorized university police officer apprehends someone for assault, she might also run the suspect's name against NCIC for operational awareness of outstanding warrants, KST status, missing person status, etc. The qualified private entities need access to NCIC to perform those functions, and do not use the information any differently than a governmental law enforcement agency. Moreover, the instructions for responding to KST hits are consistent among all criminal justice, law enforcement, and private entities with access to NCIC, regardless of the size of the entity. Someone receiving a hit on a KST record must adhere to the instructions within the returned record.[5]

Plaintiffs have requested additional information regarding why certain private entities are considered to be performing criminal justice duties as defined at 28 C.F.R. § 20.3(b), and therefore, may be eligible to apply for an ORI provided that they submit all of the required information described in the February 20, 2019 Declaration of Scott A. Rago. Specifically, Plaintiffs have asked for additional information regarding ORI eligibility by university police, hospital security, and Societies for the Prevention of Animal Cruelty (SPCAs). As stated in the Terrorist Screening Center's (TSC) Supplemental Response to Interrogatory 30, university police

[5] Further information regarding responding to a KST hit is protected by the law enforcement privilege.

departments that meet the criteria in 28 USC § 534(e)(2)[6] are authorized access to NCIC pursuant to that statute and CJIS policy. Hospital security and hospital police departments are not considered criminal justice agencies and are not issued an ORI unless they provide CJIS with the qualifying agreement they have with a governmental criminal justice agency, along with the other documentation that a private entity must submit as described in the February 20, 2019 Rago declaration. Some animal welfare organizations, such as SPCAs, have law enforcement divisions that have agreements to assist law enforcement by conducting animal cruelty investigations. Their police powers are derived from state law. Like hospital security and hospital police departments—and indeed, all entities that receive NCIC access pursuant to 28 C.F.R. § 20.33(b)—an SPCA would not be issued an ORI unless it provided CJIS, through its state CSO, with the qualifying agreement it has with a governmental criminal justice agency, along with the other required documentation showing that it is performing criminal justice services. Not all SPCA personnel would have NCIC access, but only those in the law enforcement division. This is true for any type of private entity receiving an ORI; only those individuals working in the division or subunit that performs work for a CJA will have NCIC access. Whether an SPCA, or for that matter any private entity, is for-profit or not-for-profit does not factor into whether it is eligible for an ORI, so long as the requirements for receiving an ORI are met.

During further meet and confers between counsel, Plaintiffs have requested additional information regarding how NCIC terminals operate. Historically, an NCIC terminal was a

---

[6] For both railroad police departments the police departments of private colleges and universities, these criteria are: that they (1) "perform the administration of criminal justice and have arrest powers pursuant to a State statute," (2) "allocate a substantial part of their annual budget to the administration of criminal justice," and (3) "meet training requirements established by law or ordinance for law enforcement officers."

physical piece of computer equipment used by an authorized user to access the NCIC, and each terminal was assigned a unique ORI. Terminals are in effect computers. The FBI does not provide terminals or hardware. Terminals or other hardware devices access NCIC through a regional and/or state/federal computer system. The FBI provides a host computer and telecommunication lines to a single point of contact in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada, as well as federal criminal justice agencies. That single point of contact is the state CJIS Systems Agency ("CSA"), which is typically the state's lead criminal justice agency, which is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include all local levels. Within that CSA is an individual CJIS Systems Officer ("CSO") who is responsible for the administration of the CJIS network for the CSA. Those jurisdictions, in turn, operate their own telecommunications systems, providing access to nearly all local criminal justice agencies and authorized non-criminal justice agencies nationwide. The CJIS Security Policy has strict security protocols for these systems. NCIC is not web-based and is not available or accessible on the internet. It is a machine-to-machine interface. A user, whether at a law enforcement or criminal justice agency or an authorized private entity, accesses NCIC through the CSA's network, using the ORI and other identifiers.

With respect to a question from Plaintiffs' counsel regarding "employment decisions," NCIC can only be searched for criminal justice purposes or pursuant to a federal statute, and thus cannot generally be searched by a private entity as part of a civil background check. For example, a police department at a college or a hospital cannot use NCIC to screen school applicants, students, patients, or visitors, as that is not a criminal justice purpose. As explained in the first Supplemental Response, all qualified private entities accessing NCIC are bound by

the CJIS Security Policy and CJIS Security Addendum, and are also subject to training and certification criteria, as well as audit review. Under 28 C.F.R. § 20.38, the FBI CJIS Division can cancel an ORI, effectively revoking NCIC access, if misuse is identified. A state CSA can do the same if it finds wrongdoing. Typically, however, when the CJIS Division finds a misuse or a concern, the state CSO cooperates with efforts to identify the misuse, correct it, and report back to CJIS regarding corrective measures. Individual users within an entity have been disciplined and can also face federal criminal charges for misuse or unauthorized use of a government computer system/government property.

Plaintiffs have also asked why a single private entity may receive multiple ORIs. An entity may have numerous ORIs assigned when the entity or the state/federal agency has a need to identify internal divisions, units, substations, or multiple terminals for the same agency within the same city. In addition, if an entity resides in and uses NCIC in multiple cities or states, ORIs may be assigned for each location. A qualifying private entity is not granted multiple ORIs unless it demonstrates a need to distinguish NCIC transactions by separate internal divisions, units, or substations, or that it conducts its criminal justice services in multiple locations and requests multiple ORIs.

Plaintiffs have also asked what happens when an entity that has been granted an ORI merges, is acquired, or otherwise changes corporate structure. On a biennial basis, the state/federal CSA is responsible for validating the criminal justice and law enforcement status or other valid basis for access, and all information contained within each field of the ORI File for every agency accessing the CJIS Division systems. If an entity merged or changed names, the state/federal CSA is required to gather the appropriate documentation from the entity. The state/federal CSA then forwards it to the CJIS Division for review. Depending on the

documentation, the ORI information could be modified or retired if the documentation no longer supported the qualifications under 28 USC 534 or 28 CFR Part 20. Depending on the circumstance, an existing ORI may need to be retired and a new ORI issued. With any circumstance, the state/federal CSA should be made aware and have updated agreements for a merger.

Likewise, if, for example, a college or university has a private security service but then changes the company providing that service, then the college or security service notifies the state CSA of the change, and the state CSA contacts CJIS to retire the ORI and provide the new request for a new ORI to CJIS. The purpose behind a designated state CSO within the CSA is to consolidate responsibility for ensuring compliance by all ORI users with established procedures and policies within each signatory state agency. A new ORI would be issued to the new private security service, so long as a new agreement is in place and all other requirements are met for ORI eligibility. The same process would take place if an agreement expires or is not renewed according to the specific terms of a particular agreement.[7]

Plaintiffs have also requested additional information regarding certain entities on the List. Some of the entity names on the List appeared in an abbreviated format, created by FBI CJIS OPB (or predecessor) staff, when each ORI was initially created, or subsequently updated. These names must be entered into a field in the ORI File that receives only up to a certain

[7] In the unlikely event that the state CSA is not properly notified, the state CSA would discover the change during its biennial ORI validation. In the meantime, the former security service would no longer have access to the college campus security office where the NCIC terminal is located, and therefore would no longer be able to search NCIC. The CJIS Security Addendum identifies the duties and responsibilities with respect to installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program includes consideration of personnel security, site security, system security, data security, and technical security. Moreover, an ORI alone will not grant NCIC access and other agency identifiers are also needed.

number of characters. Notwithstanding that in a few instances the abbreviated name did not indicate a police department or other explicit connection to a criminal justice function, each entity on the List is a qualified private entity, as defined above and in the February 20, 2019 Rago Declaration.

Finally, Plaintiffs requested an exhaustive list of the types of private entities that have been issued an ORI and therefore have NCIC access. As previously stated, these include: private correctional facilities; private security services for governmental facilities and hospitals; companies providing criminal justice dispatching services or data processing/information services to governmental criminal justice agencies; private probation and pretrial services companies; private city attorneys; and other entities similarly performing criminal justice services. The following is a more specific description of "other entities similarly performing criminal justice services": a private police department for an airport; a private police department for a transportation authority; private police departments for two private incorporated communities; law enforcement divisions of certain SPCAs; an inmate transport service; an entity that provides forensic services to detect and identify criminals; and court constable services.

For the Response, dated March 1, 2019:

Scott A. Rago
Acting Deputy Assistant Director
Operational Programs Branch
Criminal Justice Information Services Division
Federal Bureau of Investigation

Exhibit B

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

ANAS ELHADY, et al. Plaintiffs, v. CHARLES H. KABLE, et al. Defendants.	)	Case No. 1:16-cv-375

SECOND ADDENDUM TO SUPPLEMENTAL RESPONSE

On February 22, 2019, the Court ordered the Terrorist Screening Center (TSC) to provide a supplemental response to plaintiffs by Friday, March 1, 2019. Accordingly, the TSC provides the following second addendum to its supplemental response to Interrogatory 30 directed to the TSC and related questions at the March 1, 2018 deposition of Timothy P. Groh:

In maintaining and managing the Terrorist Screening Database (TSDB), the TSC is one of several US Government agencies committed to protecting the United States from terrorist threats and attacks. TSC disseminates TSDB information to US government agencies and officials authorized or required to conduct terrorist screening or to use information for diplomatic, military, intelligence, law enforcement, immigration, transportation security, visa, and protective processes to facilitate their respective missions. Such agencies and officials use this information in accordance with their own legal authorities. TSC's dissemination of TSDB information to other US government agencies, including the Department of Homeland Security (DHS), is pursuant to

memoranda of understanding (MOUs), and I understand all such MOUs have been provided to plaintiffs or listed on privilege logs. Each such MOU includes specific provisions governing access, disclosure, use, and security of TSDB information. TSC does not have authority to manage or oversee the screening functions of its partner agencies, but TSC is fully aware of the terms under which such information may be shared and the restrictions placed by the MOUs upon access, disclosure, and use of that information (see, e.g., MOU between TSC and TSA Regarding the Use of Terrorist Information for Security Threat Assessment Programs, provided to plaintiffs in redacted form as TSCD0063). The very purpose of these MOUs is to specify the terms by which TSDB information is shared and used. As a result, TSC can attest that its screening partners use TSDB information for lawful screening purposes, in accordance with their own legal authorities, and subject to the restrictions specified in relevant MOUs. As I have stated previously, prohibited disclosure of internal government information, let alone information protected by statutory law and privilege (such as TSDB information), constitutes a serious breach of official duties.

As a separate agency, TSC does not have comprehensive knowledge of the specific entities with which DHS components (such as the Transportation Security Administration, TSA) share TSDB information in furtherance of their missions. My First Supplemental Interrogatory Response to Interrogatory 30 ("First Supplemental Response") set forth the extent of TSC's understanding regarding how TSA may share TSDB information with "for profit" entities.

My Addendum to the First Supplemental Response ("Addendum") further explained that there are a limited number of MOUs between TSC and other US

government agencies (such as the Nuclear Regulatory Commission, Overseas Private Investment Corporation, U.S. Agency for International Development, Special Investigator General for Afghanistan Reconstruction, and the National Institute for Occupational Safety and Health) and which contain provisions regarding screening by those government agencies of personnel connected to private entities against the TSDB. My Addendum further attested that these limited number of MOUs "do not contemplate any TSDB export to private entities or access by those private entities to the TSDB." By "do not contemplate," I intended to convey that these MOUs do not provide any mechanism by which a private entity will receive a TSDB export or gain access to the TSDB. Moreover, I am not aware of any instance in which TSDB information has been shared with any private entity under any of the MOUs listed in the Addendum.

Additionally, in my First Supplemental Response, I set forth TSC's understanding that there are currently 1441 Originating Agency Identifiers (ORIs) issued to private entities that are providing services on behalf of or in support of governmental criminal justice agencies (CJA) pursuant to either 28 C.F.R. § 20.33 and 28 U.S.C. § 534 ("qualified private entities"). I further explained that the number of qualified private entities is less than 1441, because multiple ORIs have been issued to the same entity. Since my First Supplemental Response, I am advised that, after accounting for duplicate entries on the list of ORIs that plaintiffs' counsel viewed in accordance with the Court's February 22, 2019 order ("the List"), the FBI now approximates the number of qualified private entities to which ORIs have been issued to be approximately 533.[1]

1 The revised estimate is more fully explained in the concurrent supplemental response to Interrogatory 30 by the Criminal Justice Information Services (CJIS) Division of the FBI.

For the Response:

Timothy P. Groh
Deputy Director for Operations
Terrorist Screening Center

3/1/19
Date